Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE DIVISION OF RESERVE BANK OPERATIONS AND PAYMENT SYSTEMS' DISTRIBUTED PROCESSING ENVIRONMENT

OFFICE OF INSPECTOR GENERAL

(A9707) **March 1998**

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

March 4, 1998

Mr. Clyde H. Farnsworth, Jr.
Director, Division of Reserve Bank Operations and Payment Systems

We are pleased to present our *Report on the Audit of the Division of Reserve Bank Operations and Payment Systems' Distributed Processing Environment* (A9707). We performed this audit to determine if the Division of Reserve Bank Operations and Payment Systems (RBOPS) has established effective processes for planning, organizing, directing, and controlling the activities related to distributed processing; adequately managed the efficiency of its local area networks and developed an effective problem management system; properly secured its distributed systems and data; and developed appropriate backup and disaster recovery procedures.

Overall, we found that the Information Systems (IS) function within RBOPS provides responsive and high quality office automation support to the division staff. RBOPS managers and staff who responded to our survey were generally satisfied with the availability of the network and with IS' ability to resolve their technical problems. The IS staff maintains open communication with the Board's Division of Information Resources Management (IRM) and have taken steps to secure RBOPS' network and to develop a backup and recovery plan.

Notwithstanding the high quality of daily office automation support that is critical for a reliable distributed processing environment, we believe RBOPS should increase its focus on strengthening the longer-range processes of strategic planning, risk assessment and security management, and contingency planning. We also found opportunities to improve the security and general controls framework for RBOPS distributed processing and have provided our findings and recommendations to you in a separate letter for appropriate disposition. Your response, shown in appendix 1, indicates agreement with our recommendations.

A copy of this report is being sent to members of the Board's Committee on Federal Reserve Bank Affairs and selected Board staff. The report is also available on internet at *http://www.ignet.gov/ignet/internal/frb/oighome.html* and a summary will appear in our next semiannual report to Congress.

We plan to follow up on implementation of our recommendations and will report any exceptions as part of our future audit activities.

Sincerely,

Barry R. Snyder
Assistant Inspector General for Audits

Enclosure

Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE DIVISION OF RESERVE BANK OPERATIONS AND PAYMENT SYSTEMS' DISTRIBUTED PROCESSING ENVIRONMENT

OFFICE OF INSPECTOR GENERAL

(A9707) **March 1998**

TABLE OF CONTENTS

Page

BACKGROUND

Over the last several years, the Board of Governors of the Federal Reserve System (the Board) has shifted its resources to provide analytical tools to users at their desktops, while reserving larger-scale processing and storage functions for the mainframe and larger distributed servers. Shifting to the desktop computing environment offers the user a powerful set of tools for data handling; at the same time, however, operational management functions of distributed systems such as security, backup and recovery, and problem resolution and performance management may not be as fully developed as their mainframe counterparts. While these operational functions may pose potential control weaknesses, the weaknesses can be overcome by effectively managing and securing distributed office automation systems and their associated local area networks (LANs).[1]

To provide policy direction regarding the protection of its information assets, the Federal Reserve System (the System)[2] recently issued the *Information Security Manual* (ISM), which defines the security policies and safeguards for information security and is applicable to all automated platforms and manual processes throughout the System. Two additional manuals—the *Distributed Processing Security Support Manual* and the *Mainframe and FEDNET Security Support Manual*—provide more specific policies and procedures directly related to the indicated data processing environment. Board divisions and offices were expected to comply with the policies and safeguards in these manuals as of January 1, 1997.

The Division of Reserve Bank Operations and Payment Systems' Distributed Processing Environment

The Division of Reserve Bank Operations and Payment Systems (RBOPS) assists the Board and Federal Reserve Banks in promoting System objectives, which include ensuring through its oversight functions that the Reserve Banks operate effectively and efficiently, that the System provides efficient fiscal agency services to the federal agencies, and that the nation has a reliable and efficient payment mechanism. RBOPS also supports System efforts to develop strategic plans for Federal Reserve services and informs and advises the Board regarding Reserve Bank operations.

---

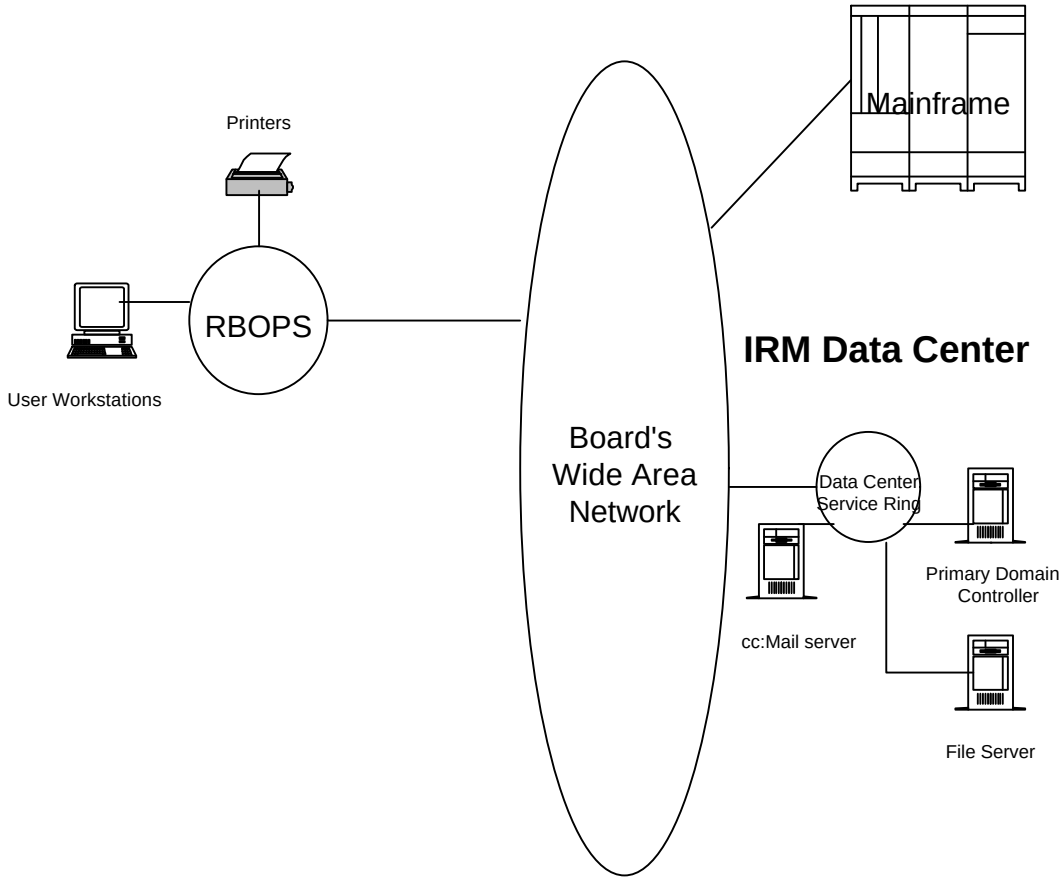
[1] A local area network (LAN) is a group of computers and other devices that are connected to exchange information and are typically dispersed throughout a small area, such as a building or office. A LAN can be connected to a larger network.

[2] "System" is used throughout the report to refer to the Board and the Federal Reserve Banks and their respective offices.

To support its mission, RBOPS has a distributed processing environment that includes two servers, one hundred fifteen LAN-connected workstations, sixteen laptops for examination staff, and thirteen network printers. Its network is a subset of the Board's wide area network, which provides connectivity to the mainframe, other LANs, the Board and System Intranets, and the Internet (see figure 1).

The RBOPS servers store data and distribute software to the division workstations for staff to use in performing office automation tasks such as word processing, spreadsheets,

Figure 1
High Level Diagram of RBOPS' Distributed Processing Environment



electronic mail and data downloading. RBOPS continues to maintain on the mainframe some data that are downloaded by RBOPS users. Through the Board's wide area network, RBOPS staff also have access to the Board's Structure Query Language (SQL), UNIX, and electronic mail servers that are administered by the Division of Information Resources

Management (IRM). RBOPS uses Microsoft's Windows New Technology (Windows NT) operating system on its workstations and Windows 95 on its laptops.

RBOPS Information Technology Management and Support Structure

The RBOPS Information Systems (IS) function administers the division's local area network, coordinates office automation systems, and develops management information systems. More specifically, IS installs, configures, and maintains the division's servers and workstations; researches, tests, evaluates, and integrates new software releases and hardware components; and handles contingency support, workstation configuration, troubleshooting, and problem resolution. IS also coordinates with IRM, which provides RBOPS with a backup and recovery system, as well as support for mainframe and InterFed connectivity.[3] The IS function's operating and capital budget totals about $900,000 for 1997, which includes four budgeted positions.

In August 1997, RBOPS merged the IS function with the Information Technology (IT) function, which promotes Federal Reserve Bank planning, evaluation, implementation, and use of information technology in an effective manner consistent with System policies. At the time of our review, the manager of the new section was considering various options to encourage information sharing between the staff assigned to each of these functions.

OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted fieldwork from August to October 1997. Our audit objectives were to determine if RBOPS has (1) established an effective process for planning, organizing, directing, and controlling the activities related to distributed processing; (2) properly secured its distributed systems and data; (3) developed appropriate backup and disaster recovery procedures; and (4) adequately managed the efficiency of its LAN and developed an effective problem management system.

To accomplish our audit objectives, we focused on the activities performed by the RBOPS IS function. We reviewed the RBOPS automation strategic plan, system configuration diagram, various system security reports, and its contingency planning document; assessed network access and security functions over the division's Windows NT network; and interviewed RBOPS officers, management, and staff. To increase our understanding of the IS function and to gain a general picture of user perceptions of RBOPS distributed process-

[3] InterFed is a wide area network that provides inter-District LAN connections for the Federal Reserve System.

ing, we distributed an office automation survey to 123 RBOPS LAN users and received 86 responses for a 70 percent response rate.[4] We also selected a judgmental sample of RBOPS workstations to observe physical security and to discuss access controls, virus protection, installed software, and backup procedures with the users. We did not review the SQL, UNIX, or electronic mail environments, since they are fully supported and administered by IRM. Our audit was conducted in accordance with generally accepted government auditing standards.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

In general, we found that the RBOPS IS function provides responsive and high quality office automation support to division staff and maintains open communication with IRM. RBOPS managers and staff who responded to our survey were generally satisfied with the availability of the network and were pleased with the responsiveness of IS staff in correcting problems. IS has also taken steps to secure the RBOPS network and to develop a backup and recovery plan.

Notwithstanding the quality of day-to-day office automation support that is critical for a reliable distributed processing environment, we believe that RBOPS should strengthen its longer-range processes of strategic planning, risk assessment and security management, and contingency planning. We also found opportunities to improve the security and general controls framework for distributed processing and have provided our findings and recommendations to the Director of RBOPS in a separate letter for appropriate disposition.

[4]We provided a summary of the survey results to RBOPS management.

1. We recommend that the Director of RBOPS develop a new automation strategic plan that will help ensure that the division's distributed processing infrastructure effectively and efficiently meets the emerging business needs of RBOPS.

The stated purpose of the existing RBOPS automation strategic plan, which is entitled *Information Systems - Strategic Direction*, is to communicate the division's information system strategy and describe why it is being pursued. According to the plan, the basic requirement for the IS function is to satisfy the current and future needs of each staff member within RBOPS. The document also notes that one of the greatest challenges for IS is to provide and integrate the requisite operating systems and hardware necessary to run the division's critical applications.

While the existing plan provides background information, it does not describe the division's long-range automation goals and objectives or specifically link the division's investment in information technology to RBOPS' mission, business goals, or System-related initiatives. The existing plan also lacks a clear and complete discussion of the internal and external environmental factors facing RBOPS distributed processing over the planning period, the potential impact of relevant IRM and System strategies to address these environmental factors, or the priorities for the division's distributed processing based upon the division's requirements and available resources.

We believe that RBOPS should develop a new automation strategic plan that addresses the division's information technology requirements, including future division and System initiatives. For instance, RBOPS is considering different ways to perform its work in overseeing Reserve Banks operations, and the strategic planning process may reveal new methods to use distributed processing to meet these demands more effectively and efficiently. With the recent merger of the IS and the IT functions, developing a new strategic plan would offer a good opportunity to set the overall direction for the section and permit it to take advantage of the skills and experiences of both groups.

Automation strategic planning may also lead RBOPS to discover even more ways to capitalize on its technology investment. In the existing plan, RBOPS recognizes that the Windows NT operating system platform provides important reliability, security, multitasking, and communications capabilities that were not available with its previous operating system. The automation strategic planning process could help RBOPS elaborate on how it will use these capabilities in supporting business requirements and enhancing its information technology infrastructure. In developing a new automation strategic plan, IS would need to consider the overall business requirements and goals of RBOPS management and staff, discuss how technology could best meet these requirements, communicate with IRM about infrastructure issues and future Boardwide directions, and coordinate with the Reserve Banks regarding their computing strategies and System initiatives.

2. We recommend that the Director of RBOPS (a) perform a risk assessment of its business functions using the ISM's standard risk assessment methodology, (b) classify its hard copy and electronic information according to the ISM, and (c) implement information security policies and controls commensurate with the resulting level of business risk.

According to the ISM, a risk assessment is the first step in establishing information security policies. The ISM requires risk assessments for all business functions to establish the applicable security controls. The System has adopted a standard risk assessment methodology that provides a systematic approach that reduces the possibility of overlooking security issues and vulnerabilities. The second step in establishing appropriate security controls under the ISM is information classification. The ISM recognizes all System information as a corporate asset that must be protected from unauthorized use or disclosure and defines information classification as a formal process of identifying, analyzing, categorizing, and inventorying information. The ISM provides a process for classifying data and handling information that is stored on electronic or printed media.

At the time of our review, RBOPS had not performed a risk assessment of its business functions or classified its information based on the corresponding risks. As a result, it cannot ensure that the security controls it has implemented for its distributed processing environment are commensurate with its level of business risk. While we noted that RBOPS has taken positive steps to implement password and other controls to meet the minimum level of policies and safeguards that the ISM recommends for a low-risk environment, additional work needs to be done to fully comply with the minimum standards. For example, security monitoring and reporting is an area where additional attention is needed. The ISM requires RBOPS to monitor unauthorized or unusual access attempts and review and reconcile security violations. While RBOPS is logging these attempts, it is not reporting or reconciling them. We believe that not meeting ISM requirements resulted from RBOPS' lack of a standard and systematic approach to setting security controls, as required and formalized by the ISM's standard risk assessment methodology.

3. We recommend that the Director of RBOPS reevaluate the division's business resumption requirements and revise the division's *Comprehensive Business Recovery Plan* to in light of its new distributed processing environment.

According to the ISM, information owners are responsible for developing, documenting, and testing a business continuity plan to help ensure that needed information is available in case of an emergency, such as hardware or software failure, inaccessibility of the building, loss of communications, or loss of the work area. The Board has a central project underway to develop a Boardwide business recovery plan and has provided divisions and offices with a software package to serve as the framework for their respective plans. Using this software package, RBOPS has prepared its *Comprehensive Business Recovery Plan*, which outlines the strategies, personnel, procedures, and resources that it plans to use to respond to any short- or long-term interruption in its essential business functions. The RBOPS plan identifies a division management team that is responsible for assessing emergencies and ensuring that the immediate critical work of the division is accomplished. It also identifies three critical mainframe applications that require immediate recovery and the quantities of some of the information technology resources that will be required in an emergency situation.

Although the RBOPS plan recognizes the division's growing reliance on distributed processing, the plan provides little information or guidance on how the distributed processing environment will be recovered. For example, the plan does not list the number and types of file servers and workstations that will be needed for business continuity, nor does it identify the critical files that will need to be recovered. Also, the time frames for recovery are broadly stated with little supporting rationale. During a short-term outage of several days or so, the plan states that the division would not restore its distributed facilities; for medium and long-range outages, it states that the cause and scope of the outage will determine the recovery strategy and does not define specific procedures for recovering distributed processing. The RBOPS plan states that in the event of an extended computer service interruption, it will implement manual processing procedures that consist of using hard copy reports and manually logging appropriate information.

We believe that RBOPS needs to reevaluate its business resumption requirements and revise its *Comprehensive Business Recovery Plan*, as necessary to specifically address recovering its distributed processing environment and operations in an cost effective, orderly and timely manner, consistent with the ISM. Distributed processing plays a major role in the everyday course of business and operating without it for even a few days would most likely have a far greater impact on operations than currently anticipated. We further caution RBOPS against overlooking the important role that distributed processing can play in facilitating business recovery in the event of an emergency. Without electronic mail capability, for example, RBOPS communication with division staff, IRM staff, Reserve Banks, and other agencies can be time consuming and difficult to coordinate. Consolidating

comments on pending legislation or regulations can be difficult to accomplish manually, as can the delivery of documents for bank activity meetings. These and other types of functions can be more efficiently accomplished using distributed processing technology, particularly when staff may be geographically dispersed during an emergency situation.

ANALYSIS OF COMMENTS

The Director of RBOPS' response to our draft report indicates general agreement with the three recommendations (see appendix 1). Specifically, he states that IS is currently developing a two year strategic plan which is consistent with the System and industry practice especially when dealing with a distributed environment. The response also indicates that IS will be performing a risk assessment and, upon completion of the assessment, will classify their data in compliance with the ISM. Finally, while RBOPS feels its current business resumption plan is suitable for its current business needs, a reevaluation of business resumption needs will be undertaken in conjunction with the risk assessment.

APPENDIXES

Appendix 1 - Division's Comments

Response to the Office of the Inspector General's
Audit of the Division of Reserve Bank Operations
And Payment Systems

Findings, Conclusions, and Recommendations

1. *The OIG recommends that the Director of RBOPS develop a new automation strategic plan that will help ensure the division's distributed processing infrastructure effectively and efficiently meets the emerging business needs of RBOPS.*

   RBOPS will comply with this recommendation. Information Systems is currently in the process of developing a two-year strategic plan. While in the past we have made an effort to develop five-year plans, it is consistent with the Federal Reserve System and the industry to reduce planning cycles to two years when dealing with distributed processing or other technical programs.

2. *The OIG recommends that the Director of RBOPS (a) perform a risk assessment of its business functions using the ISM's standard risk assessment methodology, (b) classify its hard copy and electronic information according to the ISM, and (c) implement information security policies and controls commensurate with the resulting level of business risk.*

   RBOPS will comply with this recommendation. Information System will begin working with the Information Technology program, representatives on the Board's Information Security Committee, and Division staff to formulate a Risk Assessment of the Division's data. Once complete, we will classify this data according to the ISM and implement security policies and controls congruent with the results.

3. *The OIG recommends that the Director of RBOPS reevaluate the division's business resumption requirements and revise the division's Comprehensive Business Recovery Plan in light of its new distributed processing environment.*

   RBOPS will comply with this recommendation. Information System has recently participated in a Business Recovery Plan with IRM. While we feel the results of this effort meet the Division's requirements for business resumption, RBOPS will revisit its business recovery plan in conjunction with the Division's Risk Assessment.

(A9707)

Appendix 2 - Principal OIG Contributors to this Report

Emily Drake, EDP Auditor and Auditor-in-Charge

Beth Coleman, Senior Auditor

Gary Lester, Senior EDP Auditor

Diana Falcigno, Associate EDP Auditor

Pam Debnam, Senior Secretary

Patty Kelley, Audit Manager